13 CV 6592

JUDGE BUCHWALD

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

BRIAN MOUNT and THOMAS NAIMAN,
individually and on behalf of other similarly
situated persons,

Plaintiffs,

v.

PULSEPOINT, INC.,

Defendant

Civil Action No. __________________

CLASS ACTION COMPLAINT

Jury Demand

INTRODUCTION

1. This is a consumer digital privacy class action seeking money damages and injunctive relief on behalf of Plaintiffs Thomas Naiman and Brian Mount and other similarly situated consumers (the "Class Members") domiciled in the United States who used the Apple Safari web browser ("Safari") between June 1, 2009 and February 29, 2012 (the proposed "Class Period") and visited a website that deployed third-party tracking cookies from New York-based Defendant PulsePoint, Inc. or its predecessor companies Datran Media Corp. and ContextWeb, Inc. (together, "PulsePoint").

2. Users of Safari are afforded a higher level of privacy protection than users of other browsers because Safari by default will block third party advertisers from placing cookies on their computers. Only sites actually visited by Safari users may set cookies ("first-party cookies") unless the user affirmatively changes the setting to accept third-party cookies.

3. Defendant PulsePoint, however, circumvented this privacy setting. For its own financial gain and without the knowledge or consent of Plaintiffs or other Class Members, Defendant PulsePoint illegally and secretly employed JavaScript code during the Class Period to trick the browsers on Class Members' computers, iPhones and iPads (the "Devices") into dropping the default protection and accepting tracking cookies from third-party advertisers. It was hacking in its basest form.

4. Through this hacking, PulsePoint was effectively able track the Class Members' web surfing in real time and intercept users' Internet communications and other Personally Identifiable Information ("PII"). PulsePoint then sold this illegally intercepted information to advertisers who could better target their ads to consumers based on their web surfing habits.

5. Defendants' actions thus violate various federal and New York state laws including the federal Wiretap Act and New York's consumer protection statute. In addition, Defendant knowingly and/or willfully misrepresented its privacy policy, which is also a violation of New York's consumer protection statute. [1]

6. This class action is brought on behalf of a nationwide class of Safari users whose Devices were tricked into accepting third-party tracking cookies without their consent, thus resulting in the illegal interception of Class Members' internet communications and theft of their PII. Plaintiffs bring the following causes of action:

a. Violation of New York's Consumer Protection Statute (NY GBL § 349);

b. Violation of the Federal Wiretap Act, 18 USC § 2510 *et seq*.;

c. Violation of the Stored Communications Act, 18 USC § 2701, *et seq*.;

d. Violation of the Computer Fraud and Abuse Act, 18 USC § 1030;

[1] This Complaint avers that Defendant acted knowingly and/or willfully, but specifically disclaims any claim of fraud.

e. Trespass to Chattels under New York common law; and

f. Unjust Enrichment under New York common law.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction pursuant to 28 USC § 1331 because this action arises in part under federal statutes.

8. This Court has supplemental jurisdiction over the state law claims under 28 USC § 1367(a) because they are so related to the federal claims that they form part of the same case or controversy.

9. This Court has personal jurisdiction over the Defendant because Defendant is headquartered in New York and the violations occurred in New York.

10. Venue is appropriate in this District pursuant to 28 USC § 1391(b)(1) because Defendant is headquartered in this District.

PARTIES

11. Plaintiff Brian Mount ("Mount") is an adult domiciled in the State of New Jersey who used Safari with the default settings to interact with the Internet during the Class Period for uses including review and transmitting confidential and personal information and visited websites with third-party advertisements placed by the Defendant.

12. Plaintiff Thomas Naiman ("Naiman") is an adult domiciled in the State of New York who used Safari with the default settings to interact with the Internet during the Class Period for uses including review and transmitting confidential and personal information and visited websites with third-party advertisements placed by the Defendant.

13. Defendant PulsePoint, Inc. ("Defendant" or "PulsePoint") is a digital media company which engages in consumer analytics and ad-serving across display, social, mobile,

video and email. PulsePoint is headquartered at 345 Hudson Street, New York, NY. It was formed on or about September 22, 2011, through a merger of ContextWeb, Inc. and Datran Media Corp. Both ContextWeb and Datran Media were headquartered in New York, NY. Among other lines of business, during the Class Period ContextWeb (and subsequently PulsePoint) operated an advertising exchange in which it entered into agreements with website publishers to sell advertising space on their websites, while also contracting with advertisers to place their advertisements on the publishers' websites.

FACTUAL ALLEGATIONS

A. How Web Tracking and Targeted Advertising Work

"On the Internet, nobody knows you're a dog."

©The New Yorker Collection 1993 Peter Steiner
From cartoonbank.com. All rights reserved.

14. This summer marks the 20th anniversary of the now-famous *New Yorker* cartoon (reprinted above) heralding the beginning of the internet age. The internet browser was invented in 1990 by British-born MIT professor Sir Tim Berners-Lee, which he called "WorldWideWeb," but it wasn't truly brought to the masses until 1993 with the launch of Mosaic (later Netscape).

The *New Yorker* cartoon above is the most reproduced cartoon in the magazine's history, and reflected the promise of internet anonymity and privacy in those early days.

15. Times have radically changed in the past 20 years. Today, when an internet user surfs the web, he or she is being monitored in ways unimagined by the web's inventors. The most well-known method of tracking is through the use of cookies -- small data files written to the user's browser that enable third parties to track where the user had been online. Other forms of surveillance include the use of beacons (pixel trackers), fingerprinting, and most controversially "supercookies" that can hide away from the browser and regenerate cookies even after deletion.

16. Regardless of the tracking method, all share a common purpose and origin: to generate ever-greater advertising revenues. Tracking cookies and other forms of internet surveillance enable online advertising agencies to monitor where all internet users travel online, what they do online, and when they do it, and then associate that information with other sensitive PII to create disturbingly detailed digital profiles of every internet user on earth. This information is then sold to advertisers who pay significantly higher rates to serve ads tailored precisely to the user viewing the ad.

17. When an internet user visits a website, he can either type in the address of the website or click on a link to the same address; either way, web surfing is initiated by the user's browser communicating with the server hosting the website. The browser sends a "GET" request to the server instructing the server to send data back to the browser so that the browser can construct the page for viewing.

18. Although the webpage often appears as a single “page” it is more commonly a compilation of images and other data stored on multiple servers. Messages between clients and servers are sent in internet protocol (“IP”) packets back and forth in a conversation.

19. Originally, at the beginning of the internet age, a webpage functioned as a single document, like a newspaper, with advertising incorporated into the page; these were known as “banner ads.” Today, the webpage will have one or more inline frames (iframes) which are then populated by ads placed there by ad agencies that contract to fill the frame with data normally from an entirely different server. If the user is anonymous, the frame is filled with a general ad. But if the user is known to the advertiser, it would be willing to pay far more money to target the ad to the specific user.

20. Online advertising agencies are thus strongly incentivized to gather as much personal information on each internet user as possible. Much of this is accomplished by use of cookies. Cookies are small packets of data that a website places on a user’s computer in response to the “GET” request; these identify the browser, the user, and the website. Cookies are generally classified as session cookies or persistent cookies. Session cookies are transitory and are used only to help navigate the website currently being used by the user; the cookie normally deletes when the browser closes. Persistent cookies, as the name suggests, are designed to persist even after the user moves on to a different website, or even after the browser is closed. Persistent cookies can stay on a browser for months or even years. Because persistent cookies can be read and synchronized with other cookies from the same advertizing company, they are more commonly called “tracking cookies.”

21. Commercial websites with extensive advertising – especially online content providers and publishers – contract with third parties such as Defendant to serve advertisements

in the iframes directly from the third parties' servers. Upon receiving the "GET" request from the user, the website transmits the request to the third party simultaneously with responding to the user; these communications include content, including referrer headers with search terms and other information beyond simply the identity of the user. The third party is therefore receiving instantaneous interceptions of communications between the user and first-party websites. In addition, when more than one cookie is placed on the user's Device (in a browser-managed file) from the same advertiser, the cookies can be matched and a more detailed profile can be created.

22. Therefore, given the architecture of the internet, web tracking necessarily requires the interception of electronic communications and the creation of digital profiles of each and every internet user, updated each time the user surfs the web. How society reached this point baffles many experts. Sir Berners-Lee, in addition to inventing the World Wide Web as discussed above, also invented the ubiquitous cookie which makes the modern internet possible. But he is deeply opposed to using his invention to track web users, and never intended it for that use. He has repeatedly sounded warnings about the danger. *See, e.g.*, Rory Cellan-Jones, *Web Creator Rejects Net Tracking*, BBC News (Mar. 17, 2008) (arguing that "consumers need to be protected against systems which can track their activity on the internet").

23. The public is deeply and profoundly opposed to the practice. For example, on September 5, 2013, the Pew Research Center released the results of a study called "Anonymity, Privacy and Security Online" finding that a stunning 86% of adult internet users have taken steps from time to time to avoid surveillance by other people or organizations. By far the most common strategy used by people to be less visible online (used by almost two-thirds of all internet users) is clearing cookies and browser history. The second most common strategy is setting a browser to disable or block cookies.

24. Most telling of all, internet users are far more concerned with surveillance by hackers, criminals and advertisers than by government, and the survey was taken in July 2013, two months after the recent news of NSA surveillance had already broken.

B. How Apple's Safari Browser Blocks Web Tracking and Protects Consumer Privacy

25. In 1995, Microsoft launched a browser to compete with Netscape, called "Internet Explorer," which quickly commanded a dominant position. Others followed, including Firefox and Opera. In 2003, Apple launched its own browser called Safari, which was originally confined to its customer base of Apple desktops and laptops. During the proposed Class Period, Safari accounted on average for approximately 4.1% of all desktop and laptop browsers. However, Safari became the dominant browser on mobile devices and tablets, accounting for 52.9% of all such browsers on average during the Class Period.

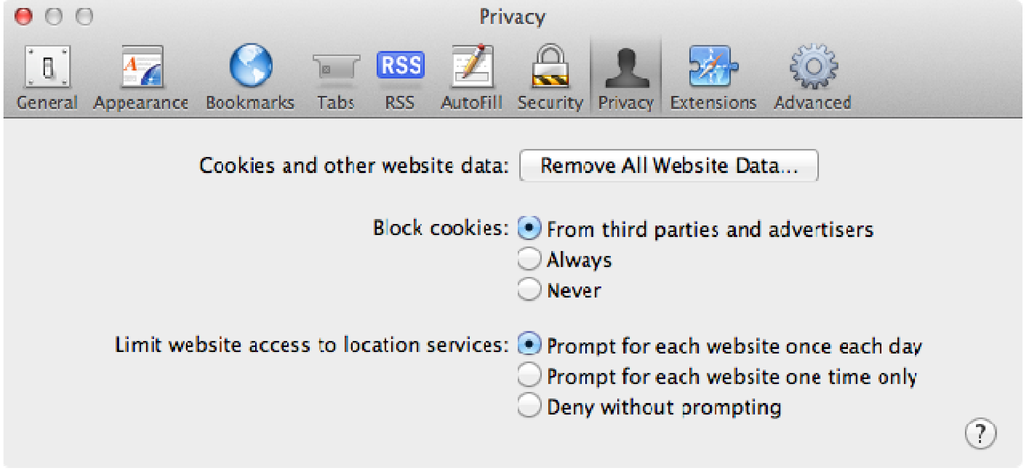
26. Sensing the public's growing awareness of web tracking and desire for increased privacy protection, Apple decided to offer third-party cookie blocking as a default setting. Millions of internet users (and, as noted above, a majority of mobile and tablet users during the Class Period) were thus protected from third-party cookies without having to find and change any setting, as would be necessary with other browsers. This privacy feature continues to be an important aspect of Apple's marketing. For example, the following language appears on Apple's website advertising Safari (current as of Sept. 12, 2013; highlighting added):

> The browser that looks out for you.
>
> **The worry-free web.**
>
> To prevent companies from tracking the cookies generated by the websites you visit, Safari blocks third-party cookies by default. It also provides built-in pop-up blocking, so you don't have to be bothered by unwanted ads.
>
> The Privacy pane in Safari preferences gives you more information about and control over your online privacy. You can see which websites are storing data that could be used to track you online.

27. On the features page of the same Apple website, Safari's default privacy setting is also touted:

> Cookie Blocking
>
> Some companies track the cookies generated by the websites you visit, so they can gather and sell information about your web activity. Safari is the first browser that blocks these tracking cookies by default, better protecting your privacy. Safari accepts cookies only from websites you visit.

28. As noted on Apple's website, Safari blocked cookies from third parties and advertisers by default:

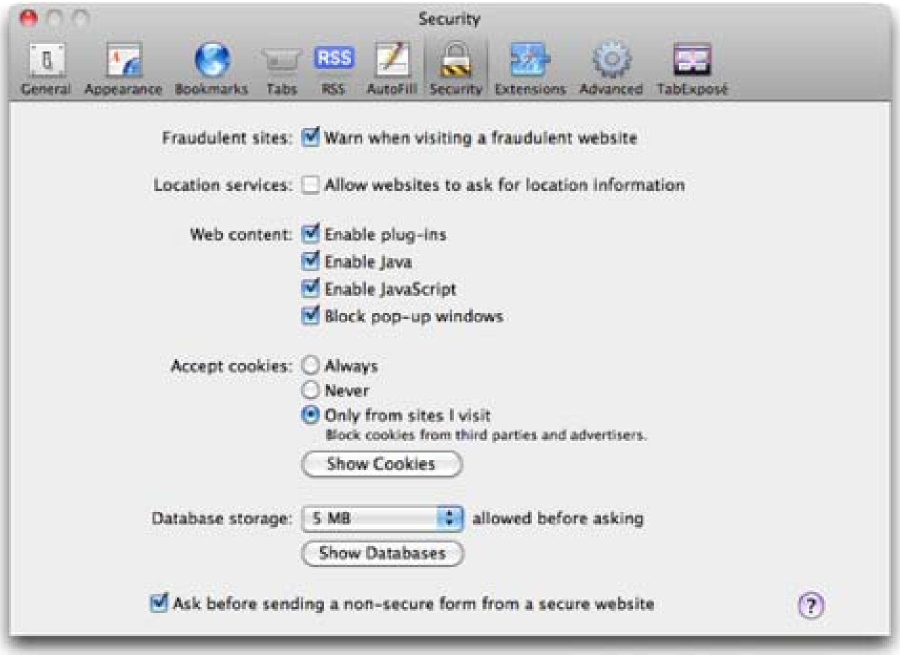


Cookies and other website data: Remove All Website Data...

Block cookies: ● From third parties and advertisers
○ Always
○ Never

Limit website access to location services: ● Prompt for each website once each day
○ Prompt for each website one time only
○ Deny without prompting

29. In earlier versions of Safari, the privacy setting appeared in a different pane ("security" not "privacy") but during the Class Period, the default setting remained the same:



Fraudulent sites: ☑ Warn when visiting a fraudulent website

Location services: □ Allow websites to ask for location information

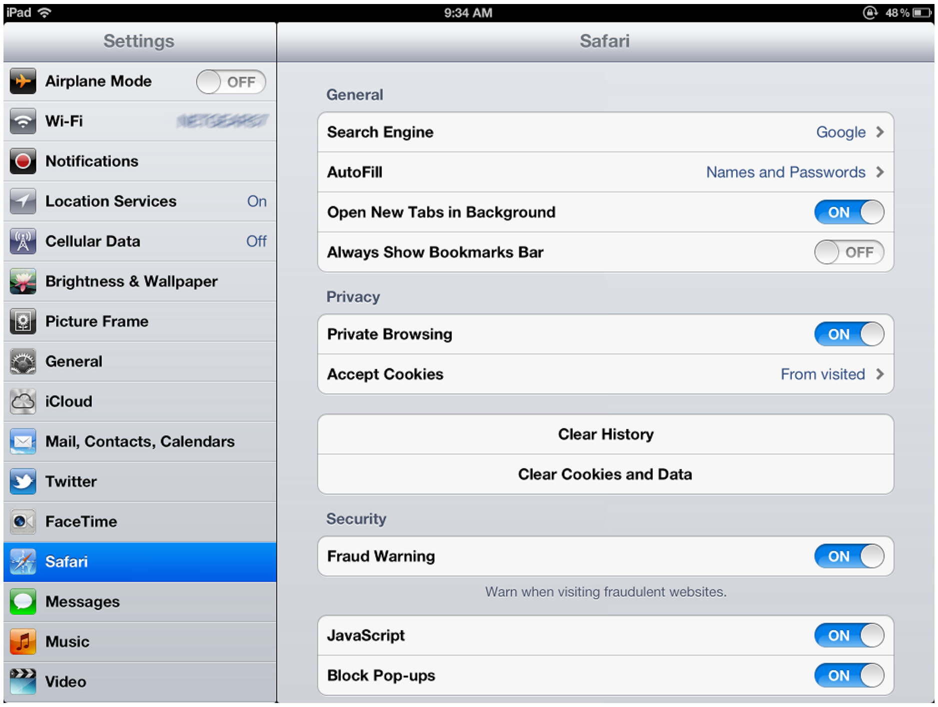
Web content: ☑ Enable plug-ins
☑ Enable Java
☑ Enable JavaScript
☑ Block pop-up windows

Accept cookies: ○ Always
○ Never
● Only from sites I visit
Block cookies from third parties and advertisers.

Database storage: 5 MB allowed before asking

☑ Ask before sending a non-secure form from a secure website

30. On iPads, Safari has the same default privacy protections, as shown here; under "Privacy," the default setting is to accept cookies only from sites visited, and other cookies are blocked:



Airplane Mode	OFF
Wi-Fi	[redacted]
Notifications	
Location Services	On
Cellular Data	Off
Brightness & Wallpaper	
Picture Frame	
General	
iCloud	
Mail, Contacts, Calendars	
Twitter	
FaceTime	
Safari	
Messages	
Music	
Video	

General

Search Engine	Google
AutoFill	Names and Passwords
Open New Tabs in Background	ON
Always Show Bookmarks Bar	OFF

Privacy

Private Browsing	ON
Accept Cookies	From visited

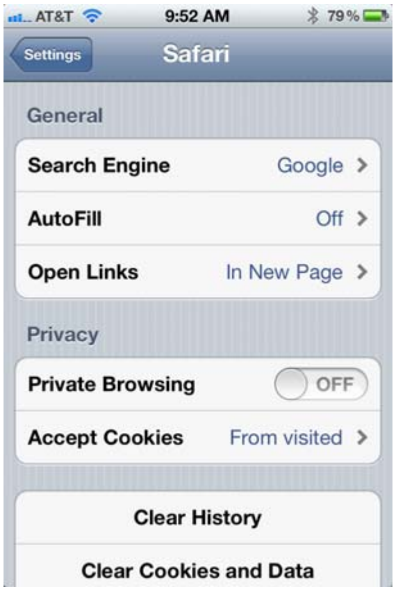
Security

Fraud Warning	ON

Warn when visiting fraudulent websites.

JavaScript	ON
Block Pop-ups	ON

31. On iPhones as well, the default privacy setting is to accept cookies only from sites visited, as shown here:



General

Search Engine: Google

AutoFill: Off

Open Links: In New Page

Privacy

Private Browsing: OFF

Accept Cookies: From visited

32. As detailed below, however, Defendant found a way to hack Safari and surreptitiously change the default settings allowing it to track users. And it was done for the most predictable of motives – money.

C. The Value of Personally Identifiable Information to Consumers ("PII") and the Cost of Web Tracking

33. The value of the personal information taken by Defendant from the Class Members and the cost of the associated tracking can be measured in four different ways.

34. **First**, and most well-known, is the value that the information has to online advertisers like the Defendant. PII has long been known as a form as currency, as noted almost 10 years ago by Harvard Law School Professor Paul Schwartz:

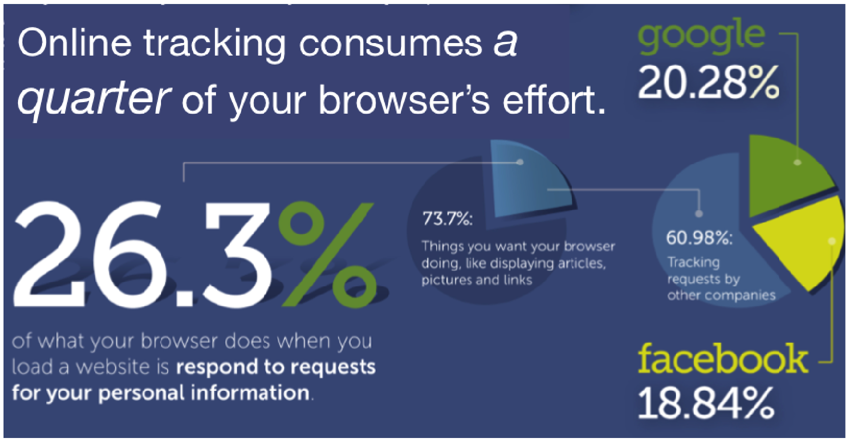
> *Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.*

Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 HARV. L. REV. 2055, 2056-57 (2004).

35. **Second**, the personal information has real monetary value to the user and can be quantified. Although the sale of users' PII originally could only be accomplished by data aggregators, individual users can now sell their PII for substantial sums of money. For example, during the Class Period Google offered web users cash in exchange for letting the user be tracked in the company's "Screenwise" program Microsoft had a similar program for its new Bing search engine (using any number of browsers, including Safari) where the company would pay users to be monitored in real time. Personal information, harvested by Defendant without any compensation to Plaintiffs, thus has real value and its theft represents real out-of-pocket loss.

36. **Third**, many users believe their information has real value far beyond the market price and will thus pay handsomely to protect it. For example, consumers currently pay various software companies to block cookies for them.

37. **Fourth and finally,** web tracking imposes substantial costs on internet users by clogging the users' Devices with hundreds of unwanted cookies, which in turn trigger a cascade of unwanted communications between the Device and various online companies. According to leading cookie-blocking software maker Abine, more than a quarter of a browser's effort is consumed by responding to requests for personal information triggered by tracking cookies implanted by companies that most users have never heard of, significantly slowing down a browser's performance and increasing CPU usage:



D. The State of New Jersey Investigation of PulsePoint, Fine and Consent Order

38. On July 23, 2013, John Hoffman, the Acting Attorney General of the State of New Jersey (the "NJ AG"), and Eric Kanefsky, the Director of the New Jersey Division of Consumer Affairs, announced an administrative action and consent order resolving an investigation by the New Jersey Division of Consumer Affairs, Office of Consumer Protection into violations by Defendant PulsePoint of the New Jersey Consumer Fraud Act ("CFA") without formal charges.

39. In sum, PulsePoint was caught hacking Safari, changing the default privacy setting of millions of Safari users without their knowledge or consent, and placing tracking cookies on their browsers. In New Jersey alone, the NJ AG estimated that the hacking enabled Defendant to deliver more than *200 million* additional illicit targeted ads.

40. In the consent order, PulsePoint admitted the following facts:

a. Between June 2009 and February 2012, PulsePoint and its predecessor ContextWeb employed a JavaScript code to place cookies on the Safari internet browsers of consumers who used Safari's default privacy setting.

b. ContextWeb's privacy policy in effect prior to August 2011 stated:

> *You can generally configure your browser to accept all cookies, reject all cookies, or notify you when a cookie is set. (Each browser is different, so check the 'Help' menu of your browser to learn how to change your cookie preferences).*

c. ContextWeb's privacy policy did not accurately describe the functionality of Safari to the public. Notwithstanding its privacy policy, ContextWeb placed cookies on the computers of users Safari whose default settings were set to block cookies from third-party advertisers.

d. Defendant, including its predecessor ContextWeb, served cookies by deploying JavaScript code in the advertisements which it placed on websites visited by consumers. ***The JavaScript code included a mechanism which replicated a submission of a form that made the Safari Browser act as if the user had clicked on the advertisement when in fact the user had not***. Once Defendant sent this form submission from the advertisement, Safari allowed Defendant to place their cookies on the Devices of users whose browsers were set to accept cookies only from "sites I visit" and "block cookies from third parties and advertisers." Defendant did not disclose to consumers that it was deploying such a mechanism.

e. One of the cookies placed by Defendant on the Devices of Class Members was a "*pb_rtb_ev*" network synchronization. This cookie was used by Defendant to allow third-party advertisement buyers to identify their cookies on Defendant's network. If the third-party buyer had also placed a cookie on the Class Member's browser, the third-party advertisement buyer was able to synchronize the consumers' cookies.

41. In the consent order, PulsePoint agreed to the following changes to its business practices:

a. PulsePoint agreed not to engage in any unfair or deceptive acts and to comply with all state and federal laws;

b. PulsePoint agreed not to change consumers' privacy settings on their browsers without their consent;

c. PulsePoint agreed not to misrepresent its data collection or use practices;

d. PulsePoint agreed to maintain systems for two years configured to instruct Safari browsers to expire any offending cookies;

e. PulsePoint agreed to update its consumer information webpage to better describe its privacy policies; and

f. PulsePoint agreed to implement a special five-year privacy program, which will include internal monitoring and an independent privacy assessment report.

42. In the consent order, PulsePoint also agreed to a settlement payment of One Million Dollars ($1,000,000.00) consisting of the following:

a. A civil penalty of $566,196.96;

b. Attorney's fees of $32,048.00;

c. Reimbursement of the NJ AG's investigative costs of $1,755.04;

d. An additional penalty of $150,000.00 to be used at the sole discretion of the NJ AG for the promotion of consumer privacy programs; and

e. An additional penalty of $250,000.00 to be used by the NJ AG for "fulfilling its statutory mission of protecting the public from fraudulent, unfair and deceptive" practices.

43. Director Kanefsky said that without PulsePoint's agreement to settle, the company would have been formally accused of violating state consumer fraud laws.[2] New Jersey Acting AG Hoffman said of the settlement with Defendant:

> ***"This settlement puts online advertisers on notice that they must respect consumers' privacy settings, or end up paying far more in penalties than any violations would generate in ad revenue."***

44. In the consent order, the NJ AG released PulsePoint from any claims the State of New Jersey could have brought under the CFA, but the release of claims explicitly carved out any private rights of action.

E. PulsePoint's Previous History of Violating Consumer Privacy Rights

45. In 2004 and 2005, Datran Media, predecessor to PulsePoint (based at PulsePoint's current address at 345 Hudson Street) purchased lists of email addresses and other private information from companies that compile such information for direct marketing purposes, including "unsolicited emails" (i.e., spam).

46. The largest such purchase at that time was a list of 7.2 million American's names, email addresses, home phone numbers and street addresses (the "personal information") from a company called Gratis Internet. However, Gratis had promised consumers that it would "never lend, sell or give out for any reason" the personal information.

[2] This Complaint avers that the Defendant acted willfully and/or knowingly but specifically disclaims any claim of fraud.

47. The New York Attorney General's office investigated Datran Media's illegal purchase of the Gratis list, and charged Datran Media along with Gratis for what the AG's office called ***the largest deliberate privacy breach in the nation's history***.

48. Datran Media originally denied knowing the details of the Gratis promise of confidentiality when it purchased the list. When the NY AG's office alleged facts establishing otherwise, Datran Media quickly settled.

49. Under the terms of the settlement, Datran Media paid a fine of $1.1 million, agreed to destroy the personal information obtained from Gratis, agreed never to purchase similar information in the future unless permitted by the consumers, and appointed a chief privacy officer to oversee compliance.

CLASS ACTION ALLEGATIONS

50. Plaintiffs bring this class action pursuant to Federal Rule of Civil Procedure 23 on behalf of a class of Internet users defined as follows:

> All persons who used Apple's Safari web browser in the United States between June 1, 2009 and February 29, 2012 and (1) whose Privacy Controls were set to block third-party advertiser cookies and (2) who visited a website that changed the Privacy Control and placed a PulsePoint, ContextWeb or Datran Media cookie on the user's Device.

51. Excluded from the Class are Defendant (including predecessor companies Datran Media and ContextWeb), their past or current officers, directors, affiliates, legal representatives, predecessors, successors, assigns and any entity in which any of them have a controlling interest, as well as all judicial officers assigned to this case as defined in 28 USC § 455(b) and their immediate families.

52. Numerosity: the Class Members are so numerous and dispersed nationwide that joinder of all members is impractical. Upon information and belief, the number exceeds several million, although the exact number is unknown.

53. Commonality: common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. These common questions include the following, among many others:

a. Whether Defendant wrote JavaScript code designed for the purpose of changing Class Members' Safari privacy settings;

b. Whether Defendant wrote the code knowingly or willfully;

c. What types of PII and web communications were intercepted due to the above acts;

d. The start and end dates of Defendant's scheme;

e. To what extent Defendant used the intercepted information for commercial gain;

f. To what extent Defendant's cookies and JavaScript code interfered with the functioning of Class Members' Devices;

g. Whether Defendant's actions violated federal law;

h. Whether Defendant's actions constituted an interception of communications "in flight,"

i. Whether Defendant's actions were materially deceptive or misleading;

j. Whether Defendant's actions occurred within the State of New York and within the United States of America;

k. Whether Defendant was aware of the Class Members whose Devices they were hacking and whether Defendant was unjustly enriched by the selling of the intercepted information; and

l. Whether the Class Members are "consumers" within the meaning of New York's consumer protection statute.

54. Typicality: Plaintiffs' claims are typical of the claims of all other Class Members. Plaintiff Naiman used Safari on his computer, while Plaintiff Mount used Safari on a mobile device. Both visited multiple websites displaying PulsePoint-arranged advertising and deploying PulsePoint cookies. Their claims are based on the same legal theories as the claims of other Class Members.

55. Adequacy: Plaintiffs will fairly and adequately protect the interests of all members of the Class in the prosecution of this action. Plaintiffs are similarly situated with, and have similar injuries to, the members of the Class they seek to represent. Both Plaintiffs are adults and have retained counsel experienced in complex class action matters generally and in the emerging field of digital privacy litigation specifically.

56. Superiority: A class action is superior to all other available methods for the fair and efficient adjudication of this case, because joinder of all members is impractical if not impossible. Furthermore, the cost of litigating each claim individually might exceed actual and/or statutory damages available to each class member thus making it impossible for each class member to litigate his or her claims individually. There will be no difficulty in managing this action as a class action.

COUNT I
Violation of New York' Consumer Protection Statute
(General Business Law § 349)

57. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

58. New York General Business Law § 349(a) prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state . . . ."

59. Defendant engaged in material, deceptive, consumer-oriented acts in the conduct of its business in this state that injured Plaintiffs and the Class in the following ways:

a. Through the degradation in value of their Devices;

b. Through the violation of their statutorily protected privacy rights; and

c. Through the theft of their PII and resale of such PII for money resulting in the unjust enrichment of Defendant.

60. As a direct and proximate result of Defendant's violation of § 349, Plaintiffs and the Class have suffered actual damages in an amount to be determined at trial.

61. Defendant willfully and/or knowingly violated § 349(a).

62. Section 349(h) provides a private right of action to enforce § 349(a) to recover each Plaintiffs' actual damages or $50 statutory damages per Class Member, whichever is greater.

63. Section 349(h) authorizes the Court to increase the amount not to exceed three times actual damages up to $1,000 per Class Member if the Court finds that Defendant willfully or knowingly violated this section.

64. Section 349(h) also authorizes the Court to award attorney's fees to a prevailing Plaintiff in addition to damages.

COUNT II
Violation of the Federal Wiretap Act
(Electronic Communications Privacy Act, 18 USC § 2510, *et seq*.)

65. Plaintiffs incorporate the above allegations by reference as if set forth fully herein

66. Defendant intentionally intercepted Plaintiffs' and the Class Members' electronic communications in flight by employing third-party tracking cookies on Class Members' Safari browsers despite the fact that Class Members were using Safari to block such interception.

67. The interception included the substance, content and/or meaning of the communications.

68. The Plaintiffs and the Class Members did not consent to the interception because they did not change the default privacy setting to accept third-party cookies.

69. Defendant's third-party web tracking permitted it to uniquely associate with their cookies detailed information about what websites a Plaintiff visited, how long he spent there, what he looked at while there, what communications were exchanged with the site, and what information had been exchanged with the site visited immediately prior.

70. As a direct and proximate result of such unlawful conduct, Defendant violated 18 USC § 2511.

71. Pursuant to 18 USC § 2520, the Court may assess statutory damages in the sum of the greater of $100.00 for each day a Class Member's electronic communications were intercepted, disclosed or used, or $10,000.00 per violation, punitive damages, injunctive or declaratory relief, and reasonable attorney's fees.

COUNT III
Violation of the Stored Communications Act, 18 USC § 2701, *et seq*. ("SCA")

72. Plaintiffs incorporate the above allegations by reference as if set forth fully herein

73. The SCA provides a private cause of action against any person who "intentionally accesses without authorization a facility through which an electronic communication service is provided," or who "intentionally exceeds an authorization to access that facility; and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in storage in such system."

74. The statute defines electronic storage as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof:" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication."

75. Defendant intentionally accessed without authorization (or intentionally exceeded authorization to access) facilities through which electronic communications systems were provided when they used the Devices to circumvent Safari's default privacy settings. Safari is by definition an "electronic communications service" under the statute.

76. Safari stores cookies and other PII in browser-managed files on the Devices. These files are "facilities" under the SCA. Access to the facilities was not authorized because Safari was set to block such access absent the Defendant's intentional hacking.

77. The cookies in the browser-managed files are regularly updated to record users' communications over the internet, including the users' browsing activities, in real time as they happen. These cookies were thus part of communications in storage, incidental to the transmission thereof.

78. The SCA, 18 USC § 2707(c), provides for the greater of actual damages caused by Defendant's violation or statutory damages of $1,000.00 per Class Member. The SCA also provides for punitive damages, costs and reasonable attorney's fees.

COUNT IV
Violation of the Computer Fraud and Abuse Act, 18 USC § 1030 ("CFAA")

79. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

80. Plaintiffs and Class Members Devices were used in interstate commerce and/or communication. Plaintiffs' web browsing, which the Defendant impermissibly tracked, involved submissions to websites across state lines.

81. The browser-managed files which were intentionally accessed by Defendant without authorization when it tricked Safari into permitting it to place and also access third-party cookies were stored on the Devices.

82. The Devices are protected computers, as defined in 18 USC § 1030(e)(2).

83. Defendant intentionally accessed the protected computers without authorization and obtained information from them in violation of 18 USC § 1030(a)(2)(c).

84. Defendant also knowingly caused the transmission of a program, information, code or command and as a result intentionally caused a loss to Plaintiffs and Class Members during a one-year period aggregating far in excess of $5,000.00 over the entire Class, in violation of 18 USC § 1030(a)(5)(a)(i).

85. Defendant also intentionally accessed the Devices without authorization and as a result caused a loss to Plaintiffs and Class Members during a one-year period aggregating far in excess of $5,000.00 over the entire Class, in violation of 18 USC § 1030(a)(5)(a)(iii).

COUNT V
Tresspass to Chattels

86. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

87. New York common law prohibits the intentional intermeddling with personal property in the possession of another that results in the deprivation of the use of the personal property or impairment of the condition, quality, or usefulness of the property.

88. Defendants dispossessed Plaintiffs and the Class Members from use and/or access to their Devices, or parts of them, without their knowledge or consent. Such acts constituted an intentional interference with the use and enjoyment of the devices.

89. More than 25% of a browser's effort is expended in dealing with third-party cookies that Class Members had every right to expect would be blocked.

90. Defendants intentionally disabled the privacy setting of the Safari browser rendering it completely useless.

91. Defendants engaged in deception to gain access to the Devices and disabling the privacy settings.

92. Plaintiffs and other Class Members thus suffered actual damages as a result of Defendant's actions in an amount to be determined at trial.

COUNT VI
Unjust Enrichment

93. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

94. Defendant PulsePoint (including its predecessor companies) illegally and without consent changed the privacy settings of Plaintiffs' Safari browsers.

95. Defendant was able to and did intercept personal and confidential web communications and other personal information and sell such personal information to third-party advertisers.

96. A market now exists for Plaintiffs to sell such information on their own.

97. There is a direct relationship between the Defendant and Plaintiffs, and indeed so direct that Defendant changed privacy settings on Plaintiffs' personal Devices and harvested personal, confidential information of Plaintiffs directly from their personal Devices for profit.

98. Defendant was enriched by its actions in New York.

99. Defendant's enrichment came at Plaintiffs' expense.

100. New York recognizes a separate common law cause of action for unjust enrichment.

101. It is against equity and good conscience to permit Defendant to retain the profits realized by the non-consensual harvest and sale of the Plaintiffs' personal information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

A. Certify this action as a Class Action pursuant to Rule 23 of the Federal Rules of Civil Procedure and appoints Plaintiffs as class representatives and their counsel as Class Counsel;

B. Award compensatory damages, including statutory damages, to Plaintiffs and the Class for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial, including interest thereon;

C. Award restitution to Plaintiffs and the Class against Defendant;

D. Award punitive damages in an amount that will deter Defendant and others from like conduct;

E. Permanently restrain Defendant and its officers, agents, employees and attorneys from violating the statutes referred to herein or otherwise violating its privacy policy and/or changing the privacy settings of any internet users' browser;

F. Award Plaintiffs the reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

G. Grant Plaintiffs such further relief as the Court deems appropriate.

JURY DEMAND

Plaintiffs demand a trial by jury of all issues triable.

Dated: September 18, 2013
New York, NY

Respectfully submitted,

KAPLAN FOX & KILSHEIMER LLP

David Straite

Frederic S. Fox
Donald R. Hall
David A. Straite
850 Third Avenue
New York, NY 10022
dstraite@kaplanfox.com
Tel.: 212.687.1980
Fax: 212.687.7714

-and-

Laurence D. King
Mario M. Choi
350 Sansome Street, Suite 400
San Francisco, CA 94104
Tel: 415.772.4700
Fax: 415.772.4707